APPENDIX D

OPERATIONS SECURITY (OPSEC)

1. Purpose. This plan prescribes policies and establishes standard procedures within the EOC for controlling and safeguarding classified material to insure that official information of the Department of Defense relating to national security is protected.

2. Applicability. This plan applies to all personnel assigned to HQUSACE.

3. Responsibilities.

a. The Chief, Emergency Operations Center (EOC), has overall responsibility for controlling and safeguarding classified material within CECW-OE-EOC.

b. The Chief of the Crisis Management Team (CMT) has the overall responsibility for controlling and safeguarding classified material in the EOC during periods when the EOC is activated with a HQUSACE CMT.

c. At a minimum, the Chief, EOC, will appoint, in writing, a security monitor who will advise on matters pertaining to the classification, declassification, and safeguarding of national security information.

d. The Chief, EOC, will implement procedures to insure that the end-of-day security check is conducted each day, IAW paragraph 5-202 of AR 380-5 and USACE Suppl 1 to AR 380-5.

e. The security monitor will:

(1) Insure that all persons who handle classified material are appropriately instructed and cleared.

(2) Assist and advise on matters pertaining to the enforcement of regulations governing the dissemination, reproduction, transmission, safe keeping, and destruction of classified material.

(3) Insure that the daily end-of-day security checks are being conducted, IAW paragraph 5-202 of AR 380-5 and USACE Suppl 1 to AR 380-5.

f. When the EOC is activated, the Clerk-Typist (Security), CMT, will:

(1) Monitor the entrance to the office and insure that all personnel who enter have been properly cleared and have the proper identification authorizing their entrance.

(2) Maintain the Restricted Area Visitor Register and issue visitor passes to properly cleared visiting personnel (see paragraph 4a. below).

g. Branch/CMT Personnel:

(1) All personnel will be familiar with and abide by instructions set forth in this plan.

(2) All personnel will be familiar with the procedures for handling and safeguarding classified materials as outlined in AR 380-5 and USACE Suppl 1 to AR 380-5.

(3) Each person is responsible for safeguarding classified documents.

(4) All CMT personnel will receive an initial security briefing by the Office of Security and Law Enforcement prior to an exercise or upon activation of the CMT. The briefing will include handling, storage, and safeguarding of classified documents.

(5) Staff assigned to the EOC will return classified material to designated GSA-approved secure containers by the end of the workday.

4. Procedures. Operations are conducted throughout the EOC at the SECRET level. Discussion of classified material is permitted in all areas except the entryway. Open storage of material is permitted during periods when the EOC is open.

a. Access to the EOC. The EOC is a restricted area and only personnel with proper security clearances will be admitted. The entrance is controlled by two locks. An electronic cipher lock ("day lock") is used for access to the EOC facility when it is open. The combination to the "day lock" may be given to all personnel with a Permanent Green EOC badge, HQUSACE General Officers and HQUSACE SES personnel. When the facility is closed a combination lock ("night lock") of the type used for GSA-approved security containers is used to double-lock the EOC. The facility can be opened and closed and the combination to the

night lock can be given only to assigned EOC staff, other Readiness Branch and section chiefs, and contiguous action officers after such personnel have been given a security orientation. Exceptions must be approved in advance by the Chief, EOC. The following procedures will be used to grant access to the area:

(1) Personnel granted access to the EOC are required to display a serially-numbered identification card in full view above the waist while in the EOC. The following types of identification cards are issued:

(a) Permanent Badge. Permanent badges (green) with photographs are issued to CMT members, Readiness Branch staff, and other individuals requiring regular, continuous access to the EOC. Holders of permanent badges must have a minimum security clearance of SECRET. A permanent badge is required in order to sign-in and escort visitors. Personnel issued a permanent badge may be given the combination to the "day lock." Permanently badged personnel will surrender badges to the EOC upon termination of their EOC/CMT assignments.

(b) Temporary Visitor Badge. Visitor "V" badges (yellow) are issued to personnel with verified minimum security clearance of SECRET and a requirement to move within the EOC without escort. Staff members issuing visitor badges are responsible for assuring security clearance has been verified against the CEPM roster or by individual verification of CEPM staff.

(c) Temporary Escort Badge. Escort "E" badges (red) are issued to personnel who require access to the EOC but do not have either the required security clearance or a need to move without an escort. Staff issuing Escort badges are responsible for escorting the badge holder at all times the individual is in the EOC. The presence of uncleared escorted visitors in the work area must be announced by the escort.

(2) Temporary badges will be issued upon surrender of photo identification (state driver's license). The photo identification will be returned in exchange for the temporary badge when the individual leaves the EOC, or at the close of business.

(3) General Officers assigned to USACE, and members of the Senior Executive Service assigned to HQUSACE and displaying blue HQUSACE SES badges, shall be given access to the EOC on the same basis as permanently badged staff. EOC badges are not required for these individuals. The EOC Administrative Officer will

regularly verify the security clearance of assigned General Officers and Senior Executives.

(4) EOC badges do not permit access to areas within the EOC which have been specifically restricted.

b. Opening and closing the EOC.

(1) Opening the EOC. The following steps shall be taken to open the EOC:

(a) Enter date/time and initials on the SF 702, Security Container Check Sheet, located on the EOC door. Turn magnetic sign to “OPEN.”

(b) Upon entering, inspect EOC perimeter, security containers, World Wide Military Command and Control System (WWMCCS) and other items listed on SF 701, Activity Security Checklist, for proper closure and/or tampering, and immediately report any problems to the Chief, EOC.

(c) Review incoming facsimile messages, and review and record telephone answering machine messages. Disseminate any information needing priority attention.

(d) A member of the permanent EOC staff shall retain responsibility for the EOC while the facility is open. As an exception, when it is essential to maintain extended operations, a member of the permanent EOC staff may temporarily leave the facility in the custody of staff with a permanent EOC badge (green). In such cases, the staff member remaining in the EOC will not leave the facility until relieved by a permanent EOC staff member.

(2) Closing the EOC. The following steps shall be taken to close the EOC:

(a) Insure that all classified material is returned to secure containers. Verify that all STU III keys are returned to a secure container.

(b) Insure that all designated equipment is turned off.

(c) Insure that all security containers are closed, checked, and the Security Container Cover Sheet, SF 702, completed.

(d) Insure that all “blocked” doorways are secure.

(e) Insure designated alarms are set.

(f) Complete Activity Security Checklist, SF 701.

(g) Set the "night lock", close the door, turn the combination dial and check the EOC door by entering the cypher lock combination.

(h) Initial the SF 702 and turn the magnetic sign to "CLOSED."

c. Safeguarding classified documents and information:

(1) During times when the EOC is activated on a 24-hour basis, classified containers may be left open to support operations. All personnel assigned to CECW-OE-EOC/CMT who handle classified information are responsible for security of the information within their control. Personnel are further responsible for insuring that any disclosure or relinquishment of control of these documents is to personnel who are properly cleared at least to the degree of the classification of the information and have a need-to-know.

(2) The dissemination of classified data orally, in writing, or by any other means, shall be limited to those persons whose official duties require knowledge or possession thereof. No one has the right to have access to classified material solely by virtue of rank or position.

(3) Classified documents may be compromised as a result of carelessness, negligence, or indiscretion, as well as by the action of hostile intelligence or subversive organizations. The dangers of indiscreet conversation cannot be over-emphasized. It is important that any breach of security which may come to an individual's attention, is reported without delay to the security monitor or supervisor. The security monitor or supervisor must be notified immediately when a document is known or suspected to be lost or compromised.

(4) Reproduction of classified material will be kept to an absolute minimum and is restricted to designated copier(s) within the EOC. In the event of equipment failure, the security office will provide guidance or assistance. Each reproduced copy of a classified document will be secured and properly controlled.

d. Storage of classified material.

(1) Each container used for storage of classified material

will be designated but not externally marked as to the level of classified material authorized to be stored. Each vault or container shall be assigned a number or symbol for identification purposes.

(2) Five containers located within the EOC are authorized storage of classified material at the SECRET level; one container is authorized for storage at the TOP SECRET level. Designated drop safes with the TOP SECRET container are provided for storage of materials requiring additional control.

(3) Combinations to classified containers will be changed only by persons having an appropriate security clearance. New combinations will be forwarded to the security office for storage. Combinations will be changed for any of the following conditions :

(a) When placed in use after procurement.

(b) Whenever an individual knowing the combination is transferred or reassigned from CECW-OE, or his/her security clearance is reduced, suspended or revoked by proper authority.

(c) When the record of combination has been compromised or the classified container was found open and unattended.

(d) At least annually, unless more frequent change is directed by the type of material stored within the container.

e. Preparation of classified documents. Classified processing is permitted only on stand-alone word processors. Data will be stored on removable hard drives and locked in GSA-approved classified containers when not in use. All documents and disks will be labeled, marked, and stored appropriately to prevent unauthorized access.

f. Emergency evacuation and destruction plan.

(1) In the event of a fire, natural disaster, or terrorist threat, the classified documents and materials stored in all safes may have to be protected, removed or destroyed. The Chief, EOC, will direct the implementation of an emergency evacuation plan, to insure that the classified documents stored in safes and containers in the EOC area are not compromised.

(2) In the event of a fire, natural disaster, or terrorist threat, the first measure of protection is to secure all containers prior to evacuating the building. The Office of

Security and Law Enforcement is subsequently responsible for implementing headquarters-wide protection procedures, to insure that containers are not breached and classified documents are not compromised during recovery and clean-up operations.

(3) If the situation warrants, destruction of the classified material will be accomplished by shredding.

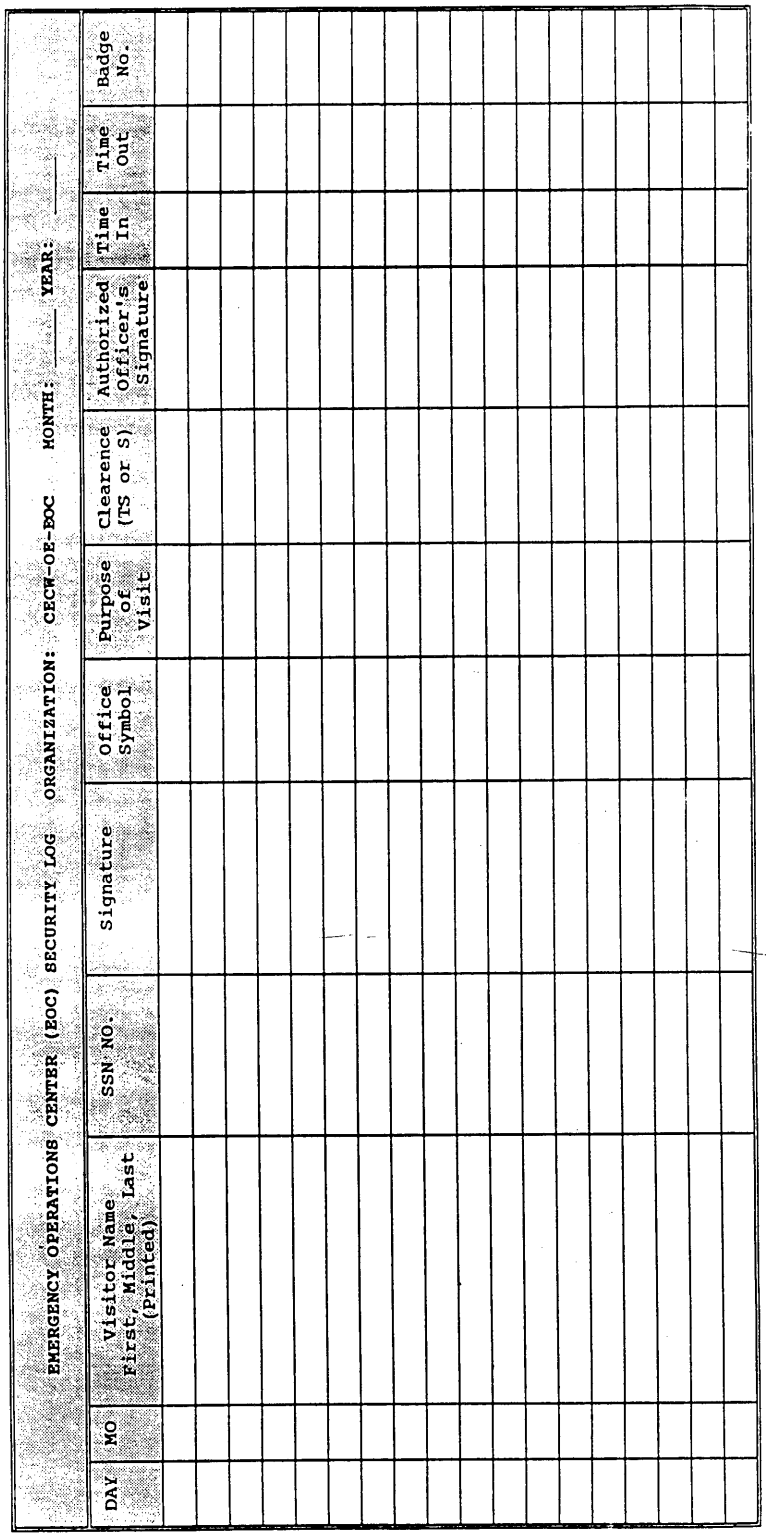
(4) Each member of CECW-OE/CMT is responsible for implementation of the emergency destruction and evacuation plan.

g. Bomb threat.

(1) If any member of the EOC/CMT team receives a bomb threat, he/she should listen as attentively as possible to the threat and record as much information as possible on the Bomb Threat Checklist (Figure D-2). Keep the bomb threat checklist readily available. A calm response to a bomb threat call may result in additional information from the caller. Pretend difficulty with your hearing and keep the caller talking.

(2) Without discussion, immediately forward the completed checklist to the Chief, EOC. The Chief, EOC will notify the Building Manager (2-0800) as soon as possible. Do not discuss the threat. Await further direction from the occupant emergency coordinator.

h. All personnel within the EOC shall consider themselves responsible for the enforcement of security procedures and regulations.



EMERGENCY OPERATIONS CENTER (EOC) SECURITY LOG ORGANIZATION: CECW-OE-EOC MONTH: _____ YEAR: _____

DAY	MO	Visitor Name First, Middle, Last (Printed)	SSN NO.	Signature	Office Symbol	Purpose of Visit	Clearence (TS or S)	Authorized Officer's Signature	Time In	Time Out	Badge No.

Figure D-1. EOC security (Register) log.

BOMB THREAT CHECKLIST

1. EXACT WORDS USED IN BOMB THREAT:_____
_____

2. TIME: _____ 3. DATE: _____ 4. DETONATION TIME: _____ 5. LOCATION: _____

6. CALLER(S):
   A. NAME:_____
   B. MALE:_____ FEMALE:_____
   C. ADDRESS:_____
   D. TELEPHONE NO.: _____
   E. THREAT MODE: _____
   F. LANGUAGE: _____ G. ACCENT :_____
   H. DIALECT: _____
   I. AGE:_____ UNKNOWN:_____ CHILD:_____ TEENAGER:_____
      YOUNG ADULT:_____ ADULT:_____ ELDER:_____

7. DID CALLER INDICATE A FAMILIARITY WITH THE BUILDING:
   YES_____ NO_____ IF YES, HOW?_____
   _____

8. ASSOCIATION:_____

9. REASON:_____

10. TYPE OF DEVICE:_____

11. MANNER OR TONE OF CALLER:_____

12. BACKGROUND NOISE:_____ 13. WEATHER:_____

13. LOCAL AREA ACTIVITY:_____

14. DAY OF WEEK: S M T W T F S PAYDAY: YES_____NO_____
    HOLIDAY:_____ WHAT DAY_____

15. MISCELLANEOUS :_____
    _____

16. RECORDER NAME:_____
    TELEPHONE NO:_____ ROOM NO:_____
    DATE:_____ TIME:_____ TITLE:_____
    AGENCY:_____ ADDRESS:_____
    _____

Figure D-2. Bomb threat checklist.